

Dieser Artikel beschäftigt sich mit Argumenten und Randbedingungen für ein WLAN. Obendrein wird auf die technische Realisierung sowie auf die Planung und Implementation einer WLAN-Struktur näher eingegangen.



# Status Quo zu Wireless LANs

ALTERNATIVE ZUR KABELGEBUNDENEN INFRASTRUKTUR?

## Gründe für ein WLAN

**Mobilität:** Dazu zwei konkrete Beispiele:

- Vertriebsmitarbeiter, die keinen festen Arbeitsplatz haben, können sich an einen beliebigen Schreibtisch im Unternehmen setzen und haben nach dem „Hochfahren“ ihres Notebooks automatisch Zugriff auf Verzeichnisse und Daten.
- In Produktionsumgebungen können sich Service-Mitarbeiter unmittelbar neben den Maschinen in das Netzwerk einloggen und somit Reparatur- und Wartungsarbeiten effektiv durchführen.

**Kostensparnis:** Grundsätzlich ist der Aufwand, eine leistungsfähige, passive und kabelgebundene Infrastruktur zu planen und einzubringen, höher als einen Firmenkomplex über mehrere WLANs zu erschließen. Das gesamte Einsparungspotential resultiert aus unterschiedlichen Faktoren:

- Verringerter Verkabelungsaufwand reduziert deutlich die Installationskosten.
- Der damit verbundene Zeitaufwand wird merklich verkürzt. Umzüge lassen sich somit dynamischer gestalten.
- Trassen können kleiner angelegt und Brandschotts der verringerten Brandlast angepaßt werden.
- Etagenverteiler, wenn sie denn noch notwendig sind,

können deutlich kleiner angelegt werden.

- Überlegungen, ob es an einzelnen Stellen zu Konzentrationen von Endgeräten kommt, entfallen. WLANs sind überall verfügbar und grundsätzlich keiner Beschränkung der Teilnehmerzahl unterworfen. Damit entfällt die Anforderung, infrastrukturelle „Überkapazitäten“ prophylaktisch bereits in der Installationsphase umsetzen zu müssen.

**Erschließung schwieriger Bereiche:** Für Bereiche, in denen die Verlegung einer herkömmlichen Tertiärverkabelung nur äußerst schwer zu realisieren wäre, kann WLAN eine passende Alternative sein:

- Produktionshallen sind aufgrund der geringen Dichte benötigter Anschlüsse im Verhältnis zur versorgenden Fläche nur sehr aufwendig zu verkabeln. Mit WLANs können Datenendgeräte vergleichsweise einfach angebunden werden. Zudem ist keine Neuverkabelung erforderlich, wenn die Produktionslinie umgestellt wird.
- Bei historischen Gebäuden sollten naturgemäß jegliche unnötigen Baumaßnahmen vermieden werden. Auch hier bieten WLANs eine adäquate Alternative zur Verkabelung.
- Abgesetzte kleine Häuser für den Werksschutz oder auch für temporäre Meßplätze

können, wenn sie nicht allzu weit entfernt stehen, über ein WLAN versorgt werden.

Hersteller rechnen mit einer Steigerung des Marktvolumens im WLAN-Bereich von heute 500 Millionen US-Dollar auf bis zu 1,6 Milliarden US-Dollar im Jahr 2005.

## Anforderungen an ein WLAN

Bei der Entwicklung einer WLAN-Technologie gibt es noch einige Schwachstellen, die vor der flächendeckenden Marktdurchdringung zufriedenstellend gelöst sein müssen.

**Interferenzen:** Bei einem WLAN werden die Daten nicht auf einer genau ausgerichteten Funkstrecke zwischen Sender und Empfänger ausgetauscht, sondern nach dem „Gießkannenprinzip“ in alle Richtungen verteilt. Durch Reflexionen an Bürowänden und -möbeln kommen gleiche Daten auf unterschiedlichen Wegen zum Empfänger. Dies führt zwangsläufig zur Überlagerung von Signalen. Der Empfänger ist nicht mehr in der Lage, die Daten auszuwerten und zu verarbeiten. Die Hersteller von WLAN-Komponenten versuchen diesen Effekt durch gerichtete Funkantennen oder aufwendige Kompensierungsverfahren zu minimieren.

**Gegenseitige Störungen:** WLAN-Übertragungen können durch andere Systeme und

Anwendungen gestört werden. Potentielle Störer sind Mikrowellen, Fahrstuhl-Generatoren, Produktionsmaschinen, Radaranlagen und natürlich auch kabellose Anwendungen wie Strichcodeleser, Bluetooth oder Funkfernbedienungen. Das Problem der Störungen wird verschärft durch die Tatsache, daß die meisten kabellosen Übertragungen das lizenzfreie 2,4-GHz-Band nutzen. Die Folgen der Behinderung reichen von einer Reduzierung der Übertragungsbandbreite bis hin zu einer nicht lauffähigen Installation. Die WLAN-Hersteller versuchen diesen negativen Auswirkungen durch entsprechende Kodierungen, verbunden mit häufigem Wechsel der Frequenz, entgegenzuwirken. Die Störung der Datenübertragung vollständig zu unterdrücken ist in den meisten Fällen jedoch nicht möglich.

Auf der anderen Seite kann ein WLAN natürlich auch als Störer auftreten und damit andere, bereits genutzte Anwendungen beeinflussen. Dies kann man verhindern, indem man im Vorfeld einer Installation die elektromagnetischen Umgebungsbedingungen mit den Verantwortlichen genau erörtert. Im Zweifelsfall können Messungen und örtlich begrenzte Teststellungen Aufschluß darüber geben, inwieweit sich zwei Funknetze gegenseitig behindern. Daß ein WLAN PCs, Produktionsmaschinen oder auch Fahrstühle

stört, ist aufgrund der geringen Sendeleistung (kleiner als ein Watt) jedoch unwahrscheinlich.

**Netzwerk-Sicherheit:** Da die Daten nicht zielgerichtet übertragen, sondern in der gesamten Funkzelle verbreitet werden, besteht die Gefahr, daß nicht autorisierte Personen Zugriff auf Unternehmensdaten bekommen. Dazu müssen diese „Spione“ sich nicht einmal auf dem Unternehmensgelände befinden. Es reicht oftmals völlig aus, sich in der Nähe eines mit WLANs ausgestatteten Gebäudes zu befinden.

Eine zweite Gefahr ist die bewußte Störung eines WLANs. Dabei wird das WLAN mit Daten überflutet, so daß das Netzwerk faktisch nicht mehr genutzt werden kann. Um dies zu verhindern, wird das in den meisten WLANs integrierte „Carrier Sense Protocol“ genutzt. Dieses Protokoll erlaubt einer Stationen erst zu senden, wenn sie das Medium als „zur Zeit frei“ erkennt. Durch einen Störer, der im WLAN ständig Daten sendet, wird das Medium von jeder Station als besetzt erkannt. Folglich wird keine Station anfangen, Daten zu übertragen.

Die Hersteller von WLAN-Produkten versuchen diese Angriffe abzuwehren, indem sie Zugangsbeschränkungen über Network Access Codes und Datenverschlüsselungsverfahren integrieren. Da in den Standards oftmals keine aus-

reichenden Sicherheitsfunktionalitäten enthalten sind, hat fast jeder Hersteller seinen Produkten proprietäre Ergänzungen hinzugefügt. Interoperabilität zwischen verschiedenen Herstellern ist bei Nutzung dieser Features natürlich nicht mehr gegeben. Leider zeigt die Praxis, daß selbst die Nutzung grundlegender Sicherheitsfunktionalitäten aufgrund des erhöhten administrativen Aufwands oftmals unterbleibt.

**Power Management:** Die Verwendung von WLAN-Netzwerkarten kann die Nutzungsdauer einer Batterie oder auch eines Akkus in einem mobilen Endgerät erheblich verkürzen. Die Hersteller von WLAN-Produkten haben daher verschiedene Verfahren implementiert, um die mögliche Arbeitszeit eines mobilen Endgeräts zu erhöhen. Beim „Schlummer-Modus“ wird in vorher festgelegten Abständen eine Mailbox abgefragt, in der Zwischenzeit bleibt die Karte inaktiv. Im Vergleich dazu wird beim „Schlaf-Modus“ die Karte nur zum Senden aktiviert – lediglich zu diesem Zeitpunkt ist das Endgerät erreichbar. Da eine Zusammenarbeit zwischen den verschiedenen Anbietern nicht zwingend gegeben ist, unterscheiden sich die Features von Hersteller zu Hersteller.

**Verbindungsprobleme:** Die möglichen Entfernungen einer Funkverbindung hängen sehr stark von den Umgebungsbedingungen ab. In einer freien

Lagerhalle sind größere Entfernungen als zwischen den Büros eines Gebäudes möglich. Leichtbauwände dämpfen das Signal geringer als stahl-armierte Wände eines Rechenzentrums. Daher müssen die Funkzellen unter Beachtung der örtlichen Gegebenheiten sehr genau geplant werden. Dabei reicht es nicht aus, daß ein Endgerät eine Verbindung aufbauen kann. Wichtig ist auch, daß die erwartete Performance erreicht wird. Diese hängt ab von der Stärke und Eindeutigkeit des Empfangssignals sowie von der Auslastung der Funkzelle. Genaue Planung hilft dieses Problem zu vermeiden. Ein anderes Verbindungsproblem entsteht, wenn sich ein mobiler Anwender zwischen verschiedenen Funkzellen bewegt. Der Übergang von einer Funkzelle in die nächste (Roaming) muß während der Planungsphase mindestens bis zur Schicht 4 des OSI-Modells durchdacht werden.

Die Schichten 1 und 2 werden durch das WLAN näher definiert. Leider ist das Roaming in den meisten Standards nicht enthalten. Die Hersteller haben aber inzwischen ihre eigenen Lösungen entwickelt. Ein herstellerreines WLAN ist für das Funktionieren dieser Lösungen in den meisten Fällen Voraussetzung. Über Interessensgemeinschaften der Hersteller wird es vielleicht zu einer gemeinsamen Roaming-Lösung kommen, die dann in die Standards einfließen kann.

## ANZEIGE

### NETZWERK- VERKABELUNG

### MALINOWSKI

In den Schichten 3 und 4 sind Protokolle wie TCP/IP für die Datenübertragung verantwortlich. Wechselt der mobile User von einem IP-Netz in das nächste, muß über Lösungen wie Mobile IP nachgedacht werden. Solche Protokolle sind jedoch nicht Bestandteil einer WLAN-Implementation.

**Gesundheitsrisiko:** Es gibt heute noch keine gesicherten Aussagen über die Auswirkungen ständiger Mikrowellen (2,4-GHz-Band) auf lebende Organismen mit einer Leistung kleiner einem Watt. Man geht jedoch davon aus, daß ein WLAN aufgrund der geringeren Sendeleistung im Vergleich zum Handy ungefährlicher ist.

**Uwe von Thienen,**  
Vorstand bei der Planungs- und Beratungsgesellschaft dvt Consulting AG, Friedrichsdorf.

**E-Mail:**  
von.Thienen@dvt-ag.de

